(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 03113657 A

(43) Date of publication of application: 15 . 05 . 91

(51) Int. Cl G06F 12/14
G06F 9/06
G09C 1/00

(21) Application number: 01253273

(22) Date of filing: 28 . 09 . 89

(71) Applicant: NEC CORP HOKKAIDO NIPPON DENKI SOFTWARE KK

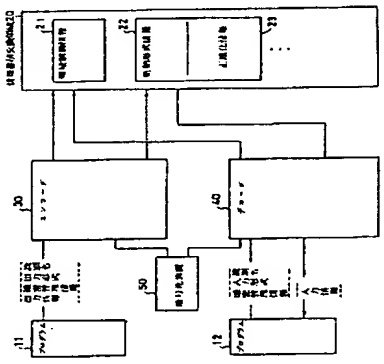
(72) Inventor: SEKINE MASAAKI
KAMOI ISAO

(54) INFORMATION ACCUMULATION EXCHANGE/SECURITY CONTROL SYSTEM

(57) Abstract:

PURPOSE: To prevent a processing from becoming complicated by providing the program with unified means for outputting and inputting information to be accumulated and exchanged and a means controlling the security of information.

CONSTITUTION: When the program 11 declares the output system of information and security control information and outputs information, an encoder 30 generates storage type information 22 from an output system, converts information into normalization information in accordance with storage type information, stores it in an information accumulation exchange area 20 and stores storage type information 22 with ciphering information 24 in the information accumulation exchange area 20. If security control information obtained by decoding ciphering information by a prescribed ciphering device and security control information which the program 12 declares are referred and they coincide when the program 12 requests the input of information, normalization information stored in the information accumulation exchange area is converted in accordance with storage type information and an input system while it is inputted to the program 12. Thus, the processing when information is accumulated and exchanged between multiple different programs is prevented from becoming complicated.



⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平3−113657

⑤Int. Cl.[5]	識別記号	庁内整理番号	㊸公開　平成3年(1991)5月15日
G 06 F 12/14	320 B	7737−5B	
9/06	450 G	7361−5B	
G 09 C 1/00		7343−5B	

審査請求　未請求　請求項の数 1　（全10頁）

㊹発明の名称　情報蓄積交換・機密管理方式

㉑特　願　平1−253273
㉒出　願　平1(1989)9月28日

㉒発明者　関根　正明　北海道札幌市中央区大通西4丁目1番地　北海道日本電気ソフトウエア株式会社内
㉒発明者　鴨井　功　東京都港区芝5丁目33番1号　日本電気株式会社内
㉑出願人　日本電気株式会社　東京都港区芝5丁目7番1号
㉑出願人　北海道日本電気ソフトウエア株式会社　北海道札幌市中央区大通西4丁目1番地
㉔代理人　弁理士　河原　純一

明　細　書

1．発明の名称

情報蓄積交換・機密管理方式

2．特許請求の範囲

互いに独立した複数のプログラムが実行される電子計算機システムのプログラム間の情報蓄積交換・機密管理方式において、

前記プログラム間で蓄積および交換される情報を格納する情報蓄積交換領域と、

第1のプログラムが前記情報の出力形式および機密管理情報を宣言して前記情報を出力したときに前記出力形式から格納形式情報を生成しこの格納形式情報に従って前記情報を正規化情報に変換して前記情報蓄積交換領域に格納するとともに前記格納形式情報を前記機密管理情報を所定の暗号化装置により暗号化した暗号化情報とともに前記情報蓄積交換領域に記録するエンコーダと、

第2のプログラムが前記情報の入力形式および機密管理情報を宣言して前記情報を入力要求したときに前記暗号化情報を所定の暗号化装置により解読した機密管理情報と第2のプログラムが宣言した機密管理情報とを照合して一致した場合に前記情報蓄積交換領域に格納された正規化情報を前記格納形式情報と前記入力形式とに従って変換しながら第2のプログラムに入力させるデコーダと

を有することを特徴とする情報蓄積交換・機密管理方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は情報蓄積交換・機密管理方式に関し、特に互いに独立な複数のプログラムが実行される電子計算機システムにおいて複数のプログラム間で情報の蓄積および交換を行う情報蓄積交換・機密管理方式に関する。

〔従来の技術〕

従来、複数のプログラム間で情報の蓄積および交換を行う場合、情報の送り手側のプログラムが受け手側のプログラムの情報の入力形式に一致させて情報を変換しながら出力する方式、情報の受け手側のプログラムが送り手側のプログラムの情

報の出力形式に一致させて情報を変換しながら入力する方式、または送り手側のプログラムと受け手側のプログラムとの間に第3のプログラムを介在させて前者の出力形式に従って出力された情報を後者の入力形式に一致する形式に変換する方式のいずれかが採用されてきた。

〔発明が解決しようとする課題〕

上述した従来の複数のプログラム間で情報の蓄積および交換を行う方式では、情報の出力形式および情報の入力形式は送り手側のプログラムおよび受け手側のプログラムのいずれか一方または双方に依存した形式となるので、以下に挙げるような欠点がある。

① 多数の異なったプログラムとの間で情報の蓄積および交換を行うプログラムの場合、相手側の個々のプログラムのそれぞれに対応する変換処理を組み込まなければならず、処理が複雑になる。

② 情報の蓄積および交換を行う相手側のプログラムが増加した場合にそれに対応してプログラムを修正しなければならない。

③ 情報の保護が十分に行われていないために、情報の出力形式を認知すれば自由に参照でき、情報の漏洩が発生する。

本発明の目的は、上述の点に鑑み、蓄積および交換される情報を出力および入力するための統一的な手段と情報の機密管理を行う手段とをプログラムに与えるようにした情報蓄積交換・機密管理方式を提供することにある。

〔課題を解決するための手段〕

本発明の情報蓄積交換・機密管理方式は、互いに独立した複数のプログラムが実行される電子計算機システムのプログラム間の情報蓄積交換・機密管理方式において、前記プログラム間で蓄積および交換される情報を格納する情報蓄積交換領域と、第1のプログラムが前記情報の出力形式および機密管理情報を宣言して前記情報を出力したときに前記出力形式から格納形式情報を生成しこの格納形式情報に従って前記情報を正規化情報に変換して前記情報蓄積交換領域に格納するとともに前記格納形式情報を前記機密管理情報を所定の暗号化装置により暗号化した暗号化情報とともに前記情報蓄積交換領域に記録するエンコーダと、第2のプログラムが前記情報の入力形式および機密管理情報を宣言して前記情報を入力要求したときに前記暗号化情報を所定の暗号化装置により解読した機密管理情報と第2のプログラムが宣言した機密管理情報とを照合して一致した場合に前記情報蓄積交換領域に格納された正規化情報を前記格納形式情報と前記入力形式とに従って変換しながら第2のプログラムに入力させるデコーダとを有する。

〔作用〕

本発明の情報蓄積交換・機密管理方式では、情報蓄積交換領域がプログラム間で蓄積および交換される情報を格納し、エンコーダが第1のプログラムが情報の出力形式および機密管理情報を宣言して情報を出力したときに出力形式から格納形式情報を生成し格納形式情報に従って情報を正規化情報に変換して情報蓄積交換領域に格納するとともに格納形式情報を機密管理情報を所定の暗号化装置により暗号化した暗号化情報とともに情報蓄積交換領域に記録し、デコーダが第2のプログラムが情報の入力形式および機密管理情報を宣言して情報を入力要求したときに暗号化情報を所定の暗号化装置により解読した機密管理情報と第2のプログラムが宣言した機密管理情報とを照合して一致した場合に情報蓄積交換領域に格納された正規化情報を格納形式情報と前記入力形式とに従って変換しながら第2のプログラムに入力させる。

〔実施例〕

次に、本発明について図面を参照して詳細に説明する。

第1図は、本発明の一実施例に係る情報蓄積交換・機密管理方式が適用された電子計算機システムの構成を示すブロック図である。この電子計算機システムは、互いに独立なプログラム11およびプログラム12と、それらの間で蓄積および交換される情報を格納するための情報蓄積交換領域20と、プログラム11が情報の出力形式等を宣言して蓄積および交換される情報を書き出したと

きに蓄積および交換される情報を格納形式情報２２および正規化情報２３に変換して情報蓄積交換領域２０に出力するエンコーダ３０と、プログラム１２が情報の入力形式等を宣言して蓄積および交換される情報を読み込もうとしたときに情報蓄積交換領域２０に格納された格納形式情報２２および正規化情報２３を入力形式に合わせて変換してプログラム１２に入力させるデコーダ４０とを含んで構成されている。

情報蓄積交換領域２０には、プログラム１１および１２間で蓄積および交換される情報の格納形式および内容を示す格納形式情報２２および正規化情報２３と、格納形式情報２２および正規化情報２３が情報の蓄積および交換を行うプログラムの組に応じて複数個存在し得るのでこれらを管理するための領域制御情報２１とが格納される。

プログラム１１が出力した蓄積および交換される情報は、エンコーダ３０が格納形式情報２２および正規化情報２３に変換して情報蓄積交換領域２０に格納する。

また、プログラム１２が受け取る蓄積および交換される情報は、情報蓄積交換領域２０に格納された格納形式情報２２および正規化情報２３をデコーダ４０が変換したものである。

第２図を参照すると、エンコーダ３０の処理は、識別名記録有無判定ステップ３０１と、格納域ポインタ取得ステップ３０２と、格納域初期化ステップ３０３と、識別名および格納域ポインタ削除ステップ３０４と、格納形式情報および暗号化情報生成ステップ３０５と、命令群構成ステップ３０６と、正規化情報生成ステップ３０７と、領域確保ステップ３０８と、格納形式情報および正規化情報出力ステップ３０９と、識別名．暗号化情報および格納域ポインタ記録ステップ３１０と、処理完了通知ステップ３１１とからなる。

第３図は、出力情報を変換して正規化情報２３を生成するための命令群を示す図である。この命令群は、エンコーダ３０によって出力形式と格納形式情報２２とから構成される。

第４図を参照すると、デコーダ４０の処理は、識別名記録有無判定ステップ４０１と、機密情報一致判定ステップ４０２と、格納域ポインタ取得ステップ４０３と、格納形式情報参照ステップ４０４と、入力形式情報生成ステップ４０５と、命令群構成ステップ４０６と、入力情報生成ステップ４０７と、入力形式情報および入力情報転送ステップ４０８と、入力情報生成完了通知ステップ４０９と、参照不可能通知ステップ４１０とからなる。

第５図は、デコーダ４０によって格納形式情報２２から入力形式に従って生成される入力形式情報の一例を示す図である。入力形式情報は、要求元のプログラム１２が宣言した入力形式を格納形式情報２２に従ってより具体化したものである。

第６図は、正規化情報２３を変換して入力情報を生成するための命令群を示す図である。この命令群は、デコーダ４０によって格納形式情報２２と入力形式情報とから構成される。

第７図は、情報蓄積交換領域２０に格納される領域制御情報２１と格納形式情報２２および正規化情報２３との関連を例示する図である。領域制御情報２１には、空領域情報と、識別名．暗号化情報２４および格納域ポインタの複数の組とが格納される。格納域ポインタは、識別名で識別される格納形式情報２２および正規化情報２３の組を指している。

第８図は、格納形式情報２２および正規化情報２３の一例をそれぞれ示す図である。格納形式情報２２内には、正規化情報２３の格納形式が定義されている。

第９図は、プログラム１１および１２からの機密管理情報の与え方を例示する図である。機密管理情報は、機密情報（パスワード）と、この機密情報（パスワード）をどのような方法で暗号化するかを指示する暗号化タイプとからなる。

第１０図は、情報蓄積交換領域２０内の領域制御情報２１に記憶される暗号化情報２４の出力例を示す図である。記憶されている機密情報（パスワード）は、暗号化タイプ「Ａ」で暗号化されたものであることを示している。

次に、このように構成された本実施例の情報蓄積交換・機密管理方式の動作について説明する。

プログラム１１は、エンコーダ３０に対する入力情報として、蓄積および交換される情報を識別するための識別名と、蓄積および交換される情報の出力形式および機密管理情報の宣言と、蓄積および交換される情報（出力情報）自身とを引き渡す。

エンコーダ３０は、まず最初に、要求元のプログラム１１が指定した識別名が領域制御情報２１内にすでに記録されているか否かをチェックする（ステップ３０１）。指定された識別名が領域制御情報２１内にすでに記録されている場合は、その識別名に対応して領域制御情報２１に記録されている格納域ポインタを得て（ステップ３０２）、格納形式情報２２および正規化情報２３が格納されている領域を初期化し（ステップ３０３）、領域制御情報２１内の識別名および格納域ポインタを削除する（ステップ３０４）。指定された識別名が領域制御情報２１内に記録されていない場合は、エンコーダ３０は、ステップ３０２～３０４を実行しない。

次に、エンコーダ３０は、要求元のプログラム１１が宣言した出力形式から格納形式情報２２を生成するとともに、プログラム１１から与えられた機密管理情報の機密情報（パスワード）を暗号化タイプから得られる暗号化装置５０により暗号化して暗号化情報２４を生成する（ステップ３０５）。さらに、出力形式とステップ３０５で生成した格納形式情報２２とを参照して、出力情報を変換して正規化情報２３を生成するための命令群を構成する（ステップ３０６）。

続いて、エンコーダ３０は、この命令群を出力情報に対して実行して正規化情報２３を生成する（ステップ３０７）。

正規化情報２３の生成後、エンコーダ３０は、領域制御情報２１を参照してステップ３０５で生成した格納形式情報２２およびステップ３０７で生成した正規化情報２３を格納するための領域を情報蓄積交換領域２０内に確保し（ステップ３０８）、格納形式情報２２および正規化情報２３を１組にして確保した領域に出力する（ステップ３０９）。

最後に、エンコーダ３０は、領域制御情報２１に、指定された識別名と、暗号化情報２４と、格納形式情報２２および正規化情報２３を格納した領域への格納域ポインタとを記録し（ステップ３１０）、要求元のプログラム１１に処理完了を通知する（ステップ３１１）。

この結果、要求元のプログラム１１が出力した蓄積および交換される情報は、格納形式情報２２および正規化情報２３に変換されて情報蓄積交換領域２０に格納される。また、格納形式情報２２および正規化情報２３が格納された領域を指示する格納域ポインタと、情報を識別するための識別名と、機密管理情報を暗号化した暗号化情報２４とが併せて領域制御情報２１内に格納される。

一方、プログラム１２は、デコーダ４０に対する入力情報として、蓄積および交換される情報を識別するための識別名と、蓄積および交換される情報の入力形式および機密管理情報の宣言と、プログラム１２内の蓄積および交換される情報を受け取るための入力域の所在情報とを引き渡す。

デコーダ４０は、まず最初に、要求元のプログラム１２が指定した識別名が領域制御情報２１内に記録されているか否かをチェックする（ステップ４０１）。指定した識別名が領域制御情報２１内に記録されていない場合には、参照不可能である旨を要求元のプログラム１２に通知する（ステップ４１０）。

また、指定した識別名が領域制御情報２１内に記録されている場合には、デコーダ４０は、プログラム１２から与えられた機密管理情報の暗号化タイプを持つ暗号化装置５０で機密情報（パスワード）を暗号化し、暗号化された機密情報（パスワード）と領域制御情報２１内の識別名に対応する暗号化情報２４の機密情報（パスワード）とを照合する（ステップ４０２）。照合が不正である場合には、参照不可能である旨を要求元のプログラム１２に通知する（ステップ４１０）。

機密情報（パスワード）の照合が一致した場合は、デコーダ４０は、識別名および暗号化情報２４とともに領域制御情報２１に記録されている格納域ポインタを得て（ステップ４０３）、格納形式情報２２を参照し（ステップ４０４）、参照した格納形式情報２２から要求元のプログラム１２が宣言した入力形式に従い入力形式情報を生成する（ステップ４０５）。

次に、デコーダ４０は、格納形式情報２２とステップ４０５で生成した入力形式情報とから、正規化情報２３を変換して入力情報を生成するための命令群を構成する（ステップ４０６）。次に、ステップ４０３で得た格納域ポインタを使用して正規化情報２３を得て、得られた正規化情報２３に対して命令群を実行して入力情報を生成する（ステップ４０７）。

続いて、デコーダ４０は、要求元のプログラム１２の蓄積および交換される情報を受け取る入力域に生成した入力情報を転送する（ステップ４０８）。

最後に、デコーダ４０は、入力情報の生成が完了したことを要求元のプログラム１２に通知する（ステップ４０９）。

なお、複数の計算機システムが通信回線等で結合されて１個のシステムを構成するような計算機システムにおいて、プログラム１１およびプログラム１２が異なった種類の中央処理装置上でそれぞれ独立に実行されているような場合でも、本発明が同様に適用できることは明白である。

〔発明の効果〕

以上説明したように本発明は、蓄積および交換される情報を出力および入力するための統一的な手段と情報の機密管理を行う手段とをプログラムに与えることにより、従来の複数のプログラム間で情報の蓄積および交換を行う方式の欠点、すなわち、

① 多数の異なったプログラムとの間で情報の蓄積および交換を行うプログラムの場合、相手側の個々のプログラムのそれぞれに対応する変換処理を組み込まなければならず、処理が複雑になる

という欠点、

② 情報の蓄積および交換を行う相手側のプログラムが増加した場合にそれに対応してプログラムを修正しなければならないという欠点、

③ 情報の保護が十分に行われていないために、情報の出力形式を認知すれば自由に参照でき、情報の漏洩が発生するという欠点

を除去することができるという効果がある。

４．図面の簡単な説明

第１図は本発明の一実施例に係る情報蓄積交換・機密管理方式が適用された電子計算機システムの構成を示すブロック図、

第２図は第１図中のエンコーダの処理を示す流れ図、

第３図は第１図中のエンコーダによって作成される命令群の一例を示す図、

第４図は第１図中のデコーダの処理を示す流れ図、

第５図は要求元のプログラムが宣言した入力形式を格納形式情報に従ってより具体化した入力形式情報の一例を示す図、

第６図は第１図中のデコーダによって作成される命令群の一例を示す図、

第７図は第１図中の情報蓄積交換領域に格納される領域制御情報と格納形式情報および正規化情報との関連を例示する図、

第８図は格納形式情報および正規化情報の一例を示す図、

第９図はプログラムからの機密管理情報の与え方を例示する図、

第１０図は第９図の機密管理情報が暗号化された暗号化情報の一例を示す図である。

図において、

１１・・・プログラム、

１２・・・プログラム、

２０・・・情報蓄積交換領域、

２１・・・領域制御情報、

２２・・・格納形式情報、

２３・・・正規化情報、

２４・・・暗号化情報、

３０・・・エンコーダ、

４０・・・デコーダ、

５０・・・暗号化装置である。

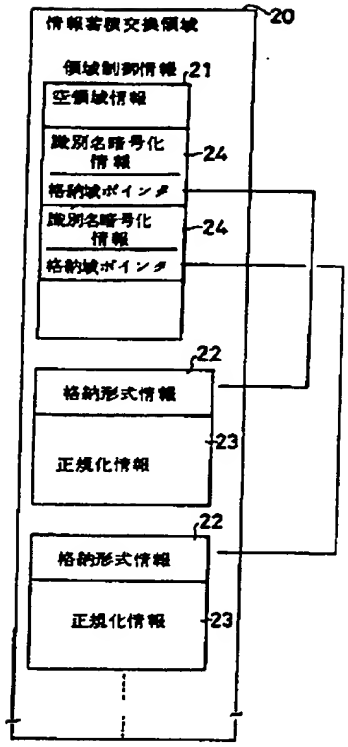
特許出願人

日本電気株式会社

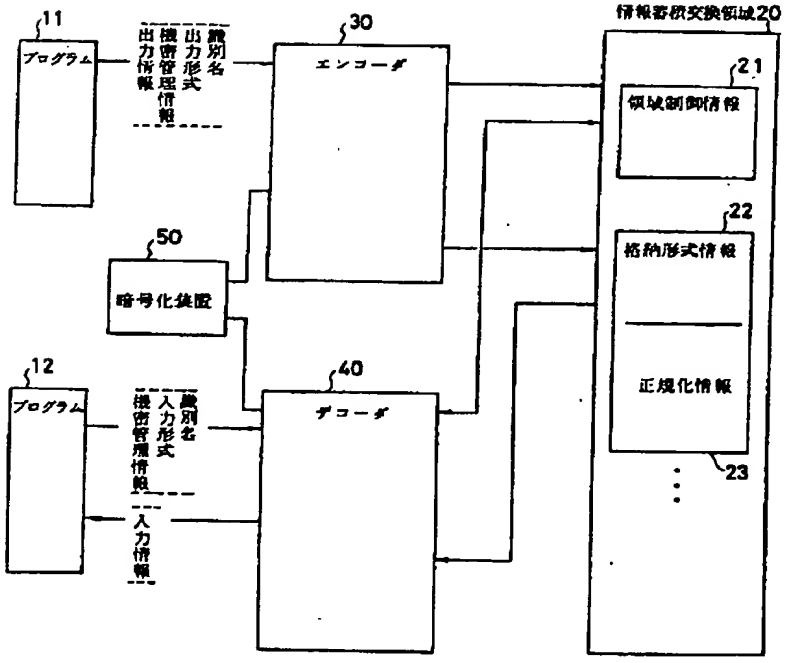
北海道日本電気ソフトウェア株式会社

代理人　弁理士　河原純一

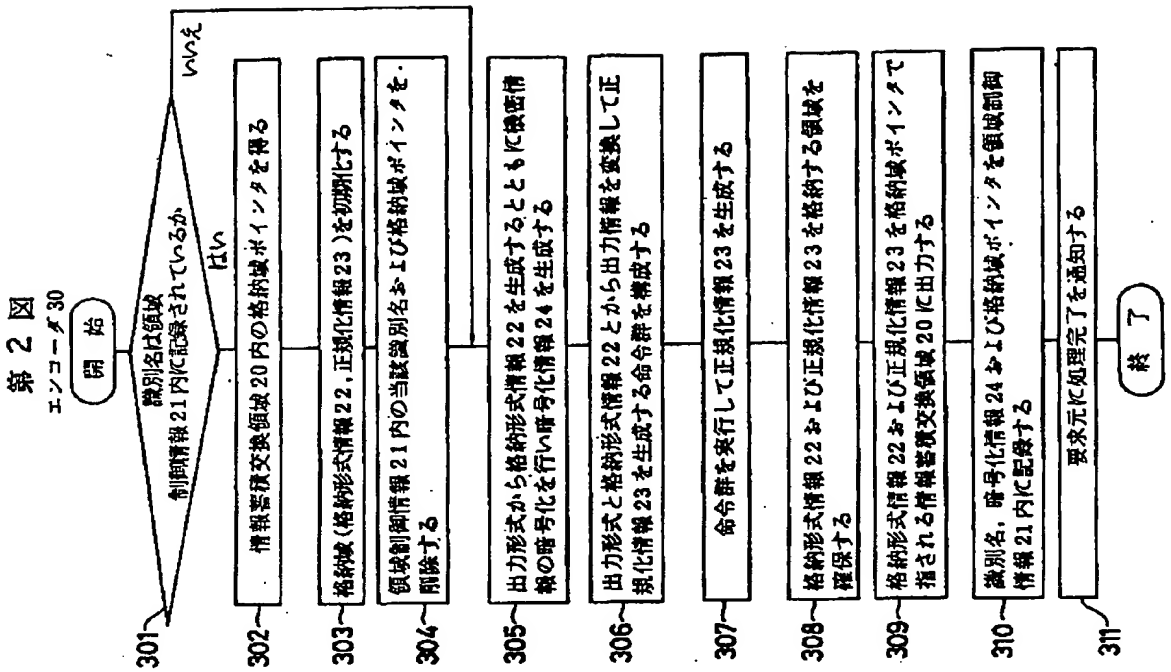
第７図



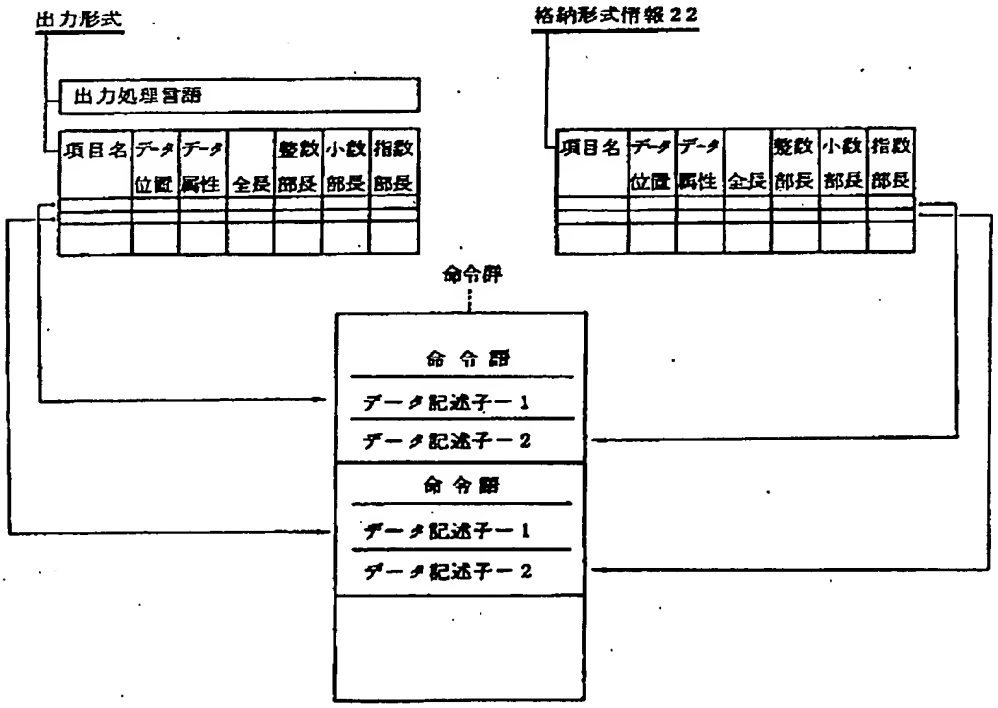
第１図



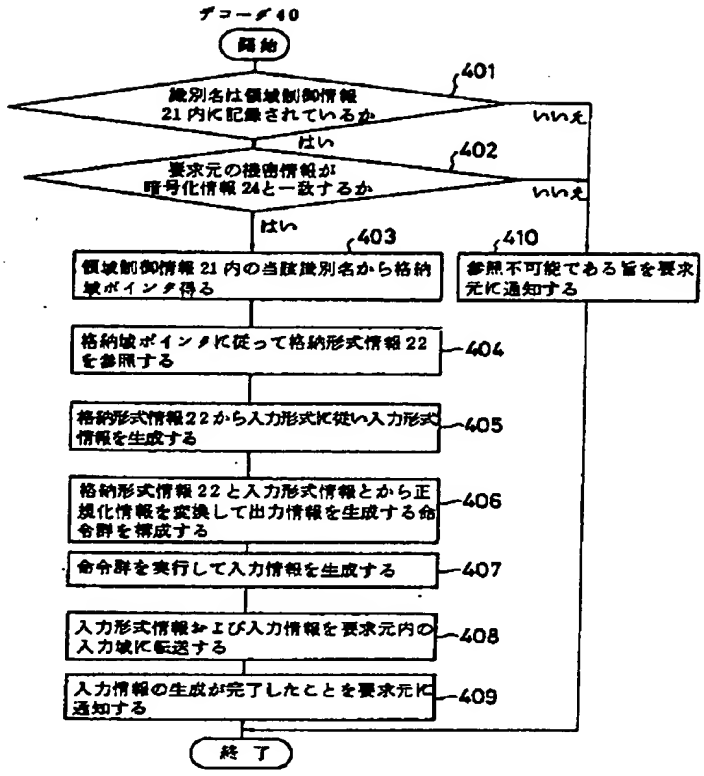
第２図


エンコーダ30
開始
識別名は領域制御情報21内に記録されているか
いいえ
はい
情報蓄積交換領域20内の格納域ポインタを得る
格納域（格納形式情報22，正規化情報23）を初期化する
領域制御情報21内の当該識別名および格納域ポインタを削除する
出力形式から格納形式情報22を生成するとともに機密情報の暗号化を行い暗号化情報24を生成する
出力形式と格納形式情報22とから出力情報を変換して正規化情報23を生成する命令群を構成する
命令群を実行して正規化情報23を生成する
格納形式情報22および正規化情報23を格納する領域を確保する
格納形式情報22および正規化情報23を格納域ポインタで指される情報蓄積交換領域20に出力する
識別名，暗号化情報24および格納域ポインタを領域制御情報21内に記録する
要求元に処理完了を通知する
終了
301
302
303
304
305
306
307
308
309
310
311

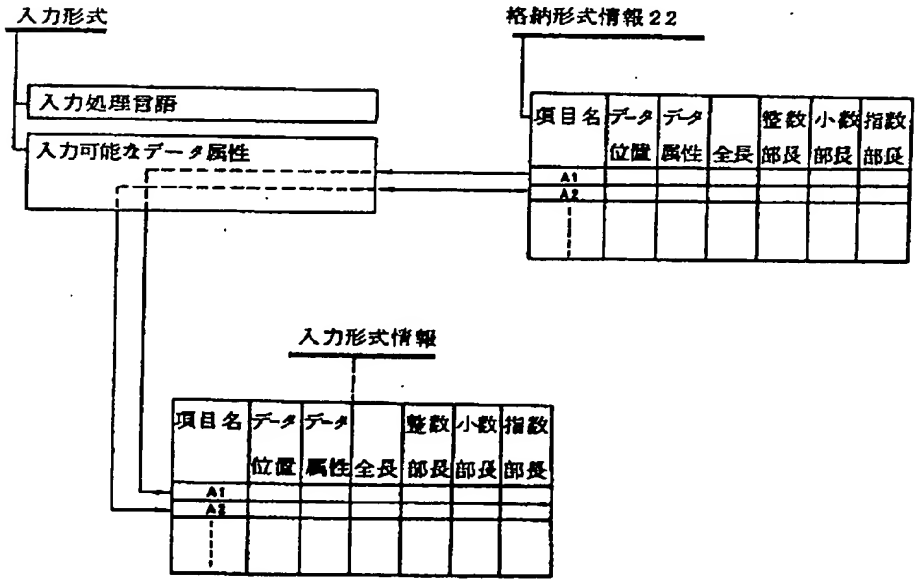
第３図


出力形式
出力処理言語
項目名
データ位置
データ属性
全長
整数部長
小数部長
指数部長
格納形式情報22
項目名
データ位置
データ属性
全長
整数部長
小数部長
指数部長
命令群
命令語
データ記述子－1
データ記述子－2
命令語
データ記述子－1
データ記述子－2

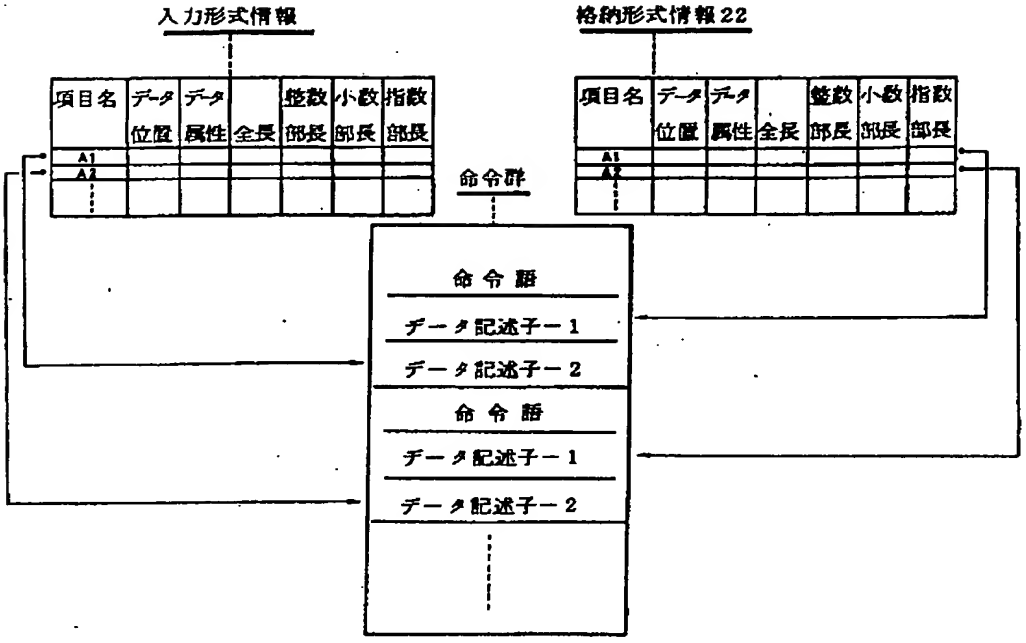
第 4 図


デコーダ40
開始
401
識別名は領域制御情報21内に記録されているか
いいえ
はい
402
要求元の機密情報が暗号化情報24と一致するか
いいえ
はい
403
領域制御情報21内の当該識別名から格納域ポインタ得る
410
参照不可能である旨を要求元に通知する
格納域ポインタに従って格納形式情報22を参照する
404
格納形式情報22から入力形式に従い入力形式情報を生成する
405
格納形式情報22と入力形式情報とから正規化情報を変換して出力情報を生成する命令群を構成する
406
命令群を実行して入力情報を生成する
407
入力形式情報および入力情報を要求元内の入力域に転送する
408
入力情報の生成が完了したことを要求元に通知する
409
終了

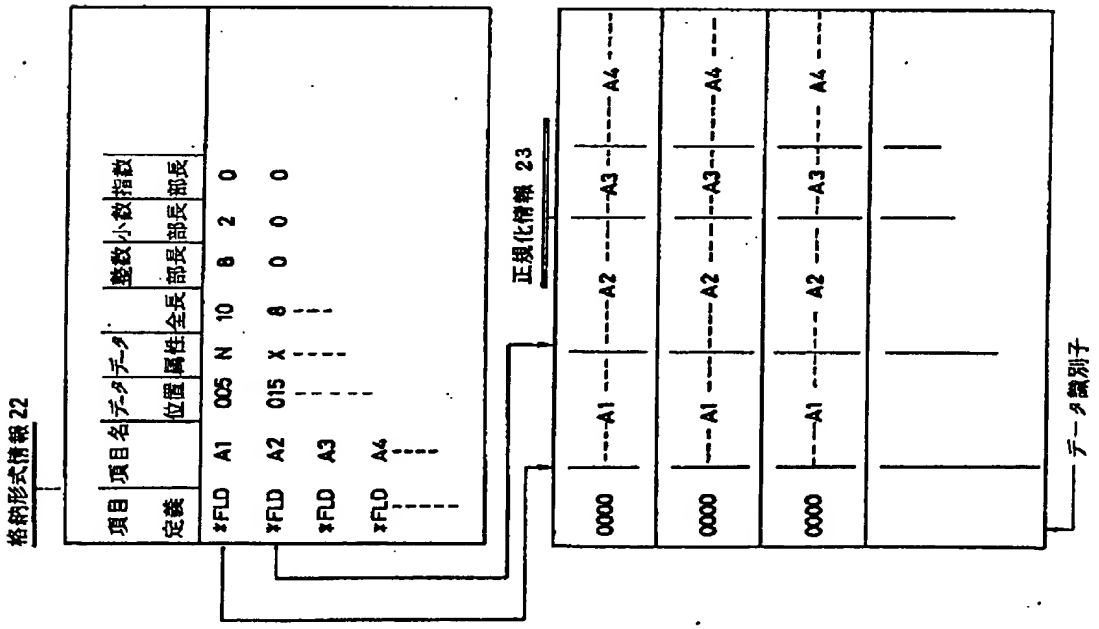
第 5 図


入力形式
入力処理冒頭
入力可能なデータ属性
格納形式情報22
項目名
データ位置
データ属性
全長
整数部長
小数部長
指数部長
A1
A2
入力形式情報
項目名
データ位置
データ属性
全長
整数部長
小数部長
指数部長
A1
A2

第 6 図


入力形式情報
格納形式情報22
項目名
データ位置
データ属性
全長
整数部長
小数部長
指数部長
A1
A2
命令群
命令語
データ記述子－1
データ記述子－2
命令語
データ記述子－1
データ記述子－2

第 8 図


格納形式情報22
項目
定義
項目名
データ位置
データ属性
全長
整数部長
小数部長
指数部長
*FLD A1 005 N 10 8 2 0
*FLD A2 015 X 8 0 0 0
*FLD A3
*FLD A4
正規化情報 23
A1
A2
A3
A4
0000
データ識別子

第 9 図

機密管理情報の与え方（プログラム11，プログラム12）

機密情報（パスワード）	＝X1X2X3X4--Xn
暗号化タイプ	＝A

第10図

暗号化情報24

項目定義	機密情報（パスワード）	暗号化タイプ
×OPT	xn---x4x3x2x1	A

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08055164 A**

(43) Date of publication of application: **27 . 02 . 96**

(51) Int. Cl **G06F 17/60**
G06F 13/00
G09C 1/00

(21) Application number: **06219369**

(22) Date of filing: **10 . 08 . 94**

(71) Applicant: **FUJITSU LTD**

(72) Inventor: **AKIYAMA RYOTA**
YOSHIOKA MAKOTO

(54) **SOFTWARE DISTRIBUTION SYSTEM, REPEATING DEVICE, AND USER TERMINAL DEVICE**

(57) Abstract:

PURPOSE: To improve the security and lighten the time load on a user by selecting the best mode for the provision style of software and perform an enciphering/deciphering process on a distribution path.

CONSTITUTION: The software which is enciphered at a center 91 is offered to a user terminal 92 through a storage medium 93 or communication media 94. When the software is offered from the center 91, the user terminal 92 refers to the accounting balance of the user and allows the software to be deciphered on condition that the balance is larger than a specific value (not 0). Then the accounting balance of the user is reduced for each title of permitted software. Then the user terminal 92 generates a deciphering key on the basis of the software ID, or title, etc., of the software and also decides the mode of the software. The user terminal 92 deciphers the software on the basis of the deciphering key and mode and outputs it to an output device such as a display and a speaker.